[6] D. K. Ray-Chaudhuri, N. M. Singhi, S. Sanyal, and P. S. Subramanian, "Theory and design of t-unidirectional error-correcting and d-unidirectional error-detecting code," *IEEE Trans. Comput.*, vol. 43, no. 10, pp. 1221–1226, Oct. 1994.

[7] J. H. Weber, C. de Vroedt, and D. E. Boekee, "Bounds and constructions for codes correcting unidirectional errors," *IEEE Trans. Inf. Theory*, vol. 35, no. 4, pp. 797–810, Jul. 1989.

[8] D. Applegate, E. M. Rains, and N. J. A. Sloane, "On asymmetric coverings and covering numbers," *J. Combin. Des.*, vol. 11, pp. 218–228, 2003.

[9] J. N. Cooper, R. B. Ellis, and A. B. Kahng, "Asymmetric binary covering codes," *J. Combin. Theory Ser. A*, vol. 100, pp. 232–249, 2002.

[10] P. R. J. Östergård and E. A. Seuranen, "Constructing asymmetric covering codes by tabu search," *J. Combin. Math. Combin. Comput.*, vol. 51, pp. 165–173, 2004.

[11] M. Krivelevich, B. Sudakov, and V. H. Vu, "Covering codes with improved density," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1812–1815, Jul. 2003.

[12] GLPK (GNU Linear Programming Kit). [Online]. Available: http://www.gnu.org/software/glpk

[13] R. G. Stanton and J. G. Kalbfleisch, "Covering problems for dichotomized matchings," *Aequationes Math.*, vol. 1, pp. 94–103, 1968.

[14] B. D. McKay, "nauty User's Guide (Version 1.5)," Comp. Sci. Depat., Australian Nat. Univ., Canberra, Tech. Rep. TR-CS-90-02, 1990.

[15] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2373–2395, Nov. 2000.

[16] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1334–1380, Nov. 1990.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[18] G. Cohen, A. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 5, pp. 680–694, Sep. 1986.

[19] D. J. Kleitman and J. Spencer, "Families of k-independent sets," *Discr. Math.*, vol. 6, pp. 255–262, 1973.

[20] G. Kéri and P. R. J. Östergård, "Further Results on the covering Radius of Small Codes," Labo. Operations Res. and Decision Syst., Computer and Automation Inst., Hungarian Acad. Sciences, Budapest, Hungary, Rep. WP 2004-1, 2004.

[21] P. R. J. Östergård, "Constructing covering codes by tabu search," *J. Combin. Des.*, vol. 5, pp. 71–80, 1997.

[22] A. Hertz, E. Taillard, and D. de Werra, "Tabu search," in *Local Search in Combinatorial Optimization*, E. Aarts and J. K. Lenstra, Eds. Chichester, U.K.: Wiley, 1997, pp. 121–136.

[23] R. Bertolo, P. R. J. Östergård, and W. D. Weakley, "An updated table of binary/ternary mixed covering codes," *J. Combin. Des.*, vol. 12, pp. 157–176, 2004.

Convolutional Goppa Codes

J. M. Muñoz Porras, *Member, IEEE*, J. A. Domínguez Pérez, J. I. Iglesias Curto, and G. Serrano Sotelo

***Abstract*—In this correspondence, we define convolutional Goppa codes over algebraic curves and construct their corresponding dual codes. Examples over the projective line and over elliptic curves are described, obtaining in particular some maximum-distance separable (MDS) convolutional codes.**

***Index Terms*—Algebraic curves, convolutional codes, finite fields, Goppa codes, maximum-distance separable (MDS) codes.**

I. Introduction

Goppa codes are evaluation codes for linear series over smooth curves over a finite field $\mathbb{F}_q$. Using Forney's algebraic theory of convolutional codes [1] (see also [2, Ch. 2] and [3]), in [4], we proposed a new construction of convolutional codes, which we called convolutional Goppa codes (CGC), in terms of evaluation along sections of a family of algebraic curves.

The aim of this correspondence is to reformulate the results of [4] in a straightforward language. In Section II, we define CGC as Goppa codes for smooth curves defined over the field $\mathbb{F}_q(z)$ of rational functions in one variable z over the finite field $\mathbb{F}_q$. These CGC are in fact more general than the codes defined in [4], since there are smooth curves over $\mathbb{F}_q(z)$ that do not extend to a family of smooth curves over the affine line $\mathbb{A}^1_{\mathbb{F}_q}$. With this definition, one has another advantage: the techniques of algebraic geometry required are easier than those used in [4]: we use exactly the same language as is usual in the literature on Goppa codes. Section III is devoted to define the dual CGC.

Section IV contains the definition of free distance for a convolutional code together with some remarks about the geometric interpretation of the Hamming weight for Goppa codes and the weight for CGC.

The last two sections of the correspondence are devoted to illustrating the general construction with some examples. In Section V we construct several CGC of genus zero; that is, defined in terms of the projective line $\mathbb{P}^1_k$ over the field $\mathbb{F}_q(z)$. Some of these examples are MDS-convolutional codes and are very easy to handle.

In Section VI, we give examples of CGC of genus one; that is, defined in terms of elliptic curves over $\mathbb{F}_q(z)$. These examples are not so easy to study. In fact, a consequence of this preliminary study of CGC of genus one is that a deeper understanding of the arithmetic properties of elliptic fibrations (see, for instance, [5]) and of the translation of these properties into the language of convolutional codes is necessary.

In the Appendix, we propose a way to obtain a geometric interpretation of the weight for CGC.

II. Convolutional Goppa Codes

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_q(z)$ the (infinite) field of rational functions of one variable. Let $(X, \mathcal{O}_X)$ be a smooth projective curve over $\mathbb{F}_q(z)$ of genus g.

Manuscript received October 14, 2003; revised November 12, 2004. This work was supported in part by the Spanish DGESYC through research Project BMF2000-1327 and by the "Junta de Castilla y León" through research Projects SA009/01 and SA032/02.

The authors are with the Department of Mathematics, University of Salamanca, 37008 Salamanca, Spain (e-mail: jmp@usal.es; jadoming@usal.es; joseig@usal.es; laina@usal.es).

Communicated by K. A. S. Abdel-Ghaffar, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.860447

Let us denote by Σ_X the field of rational functions of X and let us assume that $\mathbb{F}_q(z)$ is algebraically closed in Σ_X (this is equivalent to assuming that the fibers of the morphism π in ([4], Section 3) are geometrically irreducible curves). Both Riemann–Roch and the Residue theorems (see, for instance, [6]) still hold under this hypothesis.

Given a set $p_1, \dots, p_n$ of n different $\mathbb{F}_q(z)$-rational points of X, if $\mathcal{O}_{p_i}$ denotes the local ring at the point p_i, with maximal ideal $\mathfrak{m}_{p_i}$, and t_i is a local parameter at p_i, one has exact sequences

$$\begin{aligned} 0 \to \mathfrak{m}_{p_i} \to \mathcal{O}_{p_i} \to \mathcal{O}_{p_i}/\mathfrak{m}_{p_i} \simeq \mathbb{F}_q(z) \to 0 \\ s(t_i) \mapsto s(p_i). \end{aligned} \tag{1}$$

Let us consider the divisor $D = p_1 + \cdots + p_n$, with its associated invertible sheaf $\mathcal{O}_X(D)$. Then, one has an exact sequence of sheaves

$$0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to Q \to 0 \tag{2}$$

where the quotient Q is a sheaf with support at the points p_i.

Let G be a divisor on X of degree r, with support disjoint from D. Tensoring the exact sequence (2) by the associated invertible sheaf $\mathcal{O}_X(G)$, one obtains

$$0 \to \mathcal{O}_X(G-D) \to \mathcal{O}_X(G) \to Q \to 0. \tag{3}$$

For every divisor F over X, let us denote their $\mathbb{F}_q(z)$-vector space of global sections by

$$L(F) \equiv \Gamma(X, \mathcal{O}_X(F)) = \{s \in \Sigma_X \mid (s) + F \geq 0\}$$

where (s) is the divisor defined by $s \in \Sigma_X$. Taking global sections in (3), one obtains

$$\begin{aligned} 0 \to L(G-D) \to L(G) \xrightarrow{\alpha} \mathbb{F}_q(z) \times \overset{n}{\cdots} \times \mathbb{F}_q(z) \to \cdots \\ s \mapsto (s(p_1), \dots, s(p_n)). \end{aligned}$$

Definition 2.1: The convolutional Goppa code $\mathcal{C}(D,G)$ associated with the pair (D,G) is the image of the $\mathbb{F}_q(z)$-linear map $\alpha\colon L(G) \to \mathbb{F}_q(z)^n$.

Analogously, given a subspace $\Gamma \subseteq L(G)$, one defines the convolutional Goppa code $\mathcal{C}(D,\Gamma)$ as the image of $\alpha_{|\Gamma}$.

Remark 2.2: The above definition is more general than the one given in [4] in terms of families of curves $X \to \mathbb{A}^1_{\mathbb{F}_q}$. In fact, given such a family, the fiber X_η, over the generic point $\eta \in \mathbb{A}^1_{\mathbb{F}_q}$, is a curve over $\mathbb{F}_q(z)$. However, not every curve over $\mathbb{F}_q(z)$ extends to a family over $\mathbb{A}^1_{\mathbb{F}_q}$.

By construction, $\mathcal{C}(D,G)$ is a convolutional code of length n and dimension

$$k \equiv \dim L(G) - \dim L(G-D).$$

Proposition 2.3: Let us assume that $2g - 2 < r < n$. Then, the evaluation map $\alpha\colon L(G) \hookrightarrow \mathbb{F}_q(z)^n$ is injective, and the dimension of $\mathcal{C}(D,G)$ is

$$k = r + 1 - g.$$

Proof: If $r < n$, $\dim L(G-D) = 0$, the map α is injective and $k = \dim L(G)$. If $2g - 2 < r$, $\dim L(G) = 1 - g + r$ by the Riemann–Roch Theorem. □

III. Dual Convolutional Goppa Codes

Let us consider, over the $\mathbb{F}_q(z)$-vectorial space $\mathbb{F}_q(z)^n$, the pairing $\langle\, , \rangle$

$$\begin{aligned} \mathbb{F}_q(z)^n \times \mathbb{F}_q(z)^n &\to \mathbb{F}_q(z) \\ (u,v) &\mapsto \langle u,v\rangle = \sum_{i=1}^{n} u_i v_i \end{aligned}$$

where $u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q(z)^n$.

Definition 3.1: The dual convolutional Goppa code of the code $\mathcal{C}(D,G)$ is the $\mathbb{F}_q(z)$-linear subspace $\mathcal{C}^\perp(D,G)$ of $\mathbb{F}_q(z)^n$ given by

$$\mathcal{C}(D,G)^\perp = \{u \in \mathbb{F}_q(z)^n \mid \langle u,v\rangle = 0 \text{ for every } v \in \mathcal{C}(D,G)\}.$$

Let us denote by K the canonical divisor of rational differential forms over X.

Theorem 3.2: The dual convolutional Goppa code $\mathcal{C}^\perp(D,G)$ associated with the pair (D,G) is the image of the $\mathbb{F}_q(z)$-linear map $\beta\colon L(K+D-G) \to \mathbb{F}_q(z)^n$, given by

$$\beta(\eta) = (\mathrm{Res}_{p_1}(\eta), \dots, \mathrm{Res}_{p_n}(\eta)).$$

Proof: Following the construction of $\mathcal{C}(D,G)$, we start by tensoring the exact sequence (1) by $\mathfrak{m}^*_{p_i} = \mathrm{Hom}_{\mathcal{O}_{p_i}}(\mathfrak{m}_{p_i}, \mathcal{O}_{p_i})$, and we obtain

$$\begin{aligned} 0 \to \mathcal{O}_{p_i} \to \mathfrak{m}^*_{p_i} \to \mathcal{O}_{p_i}/\mathfrak{m}_{p_i} \otimes_{\mathcal{O}_{p_i}} \mathfrak{m}^*_{p_i} \simeq \mathbb{F}_q(z) \to 0 \\ t_i^{-1} s(t_i) \mapsto s(p_i). \end{aligned} \tag{4}$$

Again tensoring (4) by $\mathfrak{m}_{p_i}/\mathfrak{m}^2_{p_i}$, the tangent space of differentials at the point p_i, one obtains

$$\begin{aligned} 0 \to \mathfrak{m}_{p_i}/\mathfrak{m}^2_{p_i} \to \mathfrak{m}^*_{p_i} \otimes_{\mathcal{O}_{p_i}} \mathfrak{m}_{p_i}/\mathfrak{m}^2_{p_i} \to \mathbb{F}_q(z) \to 0 \\ t_i^{-1} s(t_i) dt_i \mapsto s(p_i) \end{aligned} \tag{5}$$

where $s(p_i) = \mathrm{Res}_{p_i}(t_i^{-1} s(t_i) dt_i)$.

This allows us to define a new convolutional Goppa code associated with the pair of divisors $D = p_1 + \ldots + p_n$ and G; tensoring (2) by the line sheaf $\mathcal{O}_X(K+D-G)$, one has

$$0 \to \mathcal{O}_X(K-G) \to \mathcal{O}_X(K+D-G) \to Q \to 0. \tag{6}$$

Taking global sections, one has

$$\begin{aligned} 0 \to L(K-G) \to L(K+D-G) \xrightarrow{\beta} \mathbb{F}_q(z) \times \overset{n}{\cdots} \times \mathbb{F}_q(z) \to \ldots \\ \eta \mapsto (\mathrm{Res}_{p_1}(\eta), \dots, \mathrm{Res}_{p_n}(\eta)). \end{aligned}$$

The image of β is a subspace of $\mathbb{F}_q(z)^n$, whose dimension can be calculated by the Riemann–Roch theorem

$$\begin{aligned} &\dim L(K+D-G) - \dim L(K-G) \\ &= \dim L(G-D) - (r-n) - 1 + g - (\dim L(G) - r - 1 + g) \\ &= n - k. \end{aligned}$$

Moreover, $\mathcal{I}\mathrm{m}\beta$ is the subspace $\mathcal{C}(D,G)^\perp \subset \mathbb{F}_q(z)^n$, since they have the same dimension, and for every $\eta \in L(K+D-G)$ and every $s \in L(G)$ one has

$$\langle \beta(\eta), \alpha(s)\rangle = \sum_{i=1}^{n} s(p_i)\mathrm{Res}_{p_i}(\eta) = \sum_{i=1}^{n} \mathrm{Res}_{p_i}(s\eta) = 0$$

by the Residue theorem. □

Under the hypothesis $2g-2<r<n$, the map β is injective, and $\mathcal{C}^{\perp}(D,G)$ is a convolutional code of length n and dimension

$$\dim L(K+D-G)=n-(1-g+r).$$

Remark 3.3: Our pairing $\langle\,,\rangle\colon \mathbb{F}_q(z)^n\times\mathbb{F}_q(z)^n\to\mathbb{F}_q(z)$ is $\mathbb{F}_q(z)$-bilinear, whereas the "time reversal" pairing defined by Rosenthal in [7, Sec. 7.2], given by

$$[\,,]\colon \mathbb{F}_q((z))^n\times\mathbb{F}_q((z))^n\to\mathbb{F}_q$$

$$(u,v)\mapsto\sum_{i=1}^{n}\langle u(i),v(-i)\rangle$$

where $u=\sum_i u(i)z^i, v=\sum_i v(i)z^i\in\mathbb{F}_q((z))^n$ and $\langle\,,\rangle$ is the standard bilinear form on $\mathbb{F}_q^n$, is $\mathbb{F}_q$-bilinear.

The pairing $[\,,]$ can be expressed in the following way:

$$[u,v]=\mathrm{Res}_{z=0}\left(\langle u,v\rangle\frac{dz}{z}\right)=\sum_{i=1}^{n}\mathrm{Res}_{z=0}\left(u_iv_i\frac{dz}{z}\right).$$

Thus, the duality for convolutional Goppa codes in Definition 3.1 is related to the residues in the points of X, and the duality with respect to the pairing $[\,,]$ is related to the residues in the variable of the base field. Accordingly, a more precise study of the relationship between both dualities must be done.

IV. Minimum Distance and Free Distance

Given a vector $u=(u_1,\dots,u_n)\in\mathbb{F}_q^n$, its weight is defined as $\mathrm{wt}(u)=\#\{i\,|\,u_i\neq 0\}$. The minimum weight (minimum distance) of a linear block code is one of the most important parameters in the theory of linear block codes.

For polynomial vectors one has the possibility of defining two kinds of weights. Let us consider a polynomial vector

$$u=(u_1,\dots,u_n)\in\mathbb{F}_q[z]^n\subset\mathbb{F}_q((z))^n,\quad\text{where } u_i\in\mathbb{F}_q[z].$$

We can also represent the vector u as a polynomial with vector coefficients

$$u=\sum_i u(i)z^i,\quad\text{where}\quad u(i)\in\mathbb{F}_q^n.$$

One can define the Hamming weight of u as

$$h\mathrm{wt}(u)=\#\{i\,|\,u_i\neq 0\}.$$

The minimum Hamming weight of a convolutional code does not reflect the performance of convolutional codes over noisy channels in convolutional coding theory. Of course the minimum Hamming weight of a convolutional Goppa code $\mathcal{C}(D,G)$ can be bounded using the Riemann–Roch Theorem, as in the usual Goppa codes.

The natural notion of weight in convolutional coding theory is as follows

$$\mathrm{wt}(u)=\sum_i\mathrm{wt}(u(i)).$$

The free distance of a convolutional code $\mathcal{C}\subseteq\mathbb{F}_q[z]^n$ is defined by

$$d_{\text{free}}=\min\{\mathrm{wt}(u)\,|\,u\in\mathcal{C},\ u\neq 0\}.$$

This is one of the most important parameters in convolutional coding theory.

The geometric interpretation of the Hamming weight for Goppa codes in terms of the number of zeroes of certain meromorphic functions allows use of the Riemann–Roch Theorem to make very precise computations. In the case of convolutional Goppa codes the interpretation of the notion of weight in geometrical terms is much more difficult.

In the Appendix, we propose a way to obtain a geometric interpretation of the weight in terms of osculating planes to the algebric curve.

In the next two sections we construct some examples of convolutional Goppa codes. The free distance is computed in terms of the generator matrix using symbolic calculus software.

V. Convolutional Goppa Codes Over the Projective Line

Let $X=\mathbb{P}^1_{\mathbb{F}_q(z)}=\mathrm{Proj}\mathbb{F}_q(z)[x_0,x_1]$ be the projective line over the field $\mathbb{F}_q(z)$, and let us denote by $t=x_1/x_0$ the affine coordinate.

Let $p_0=(1,0)$ be the origin point, $p_\infty=(0,1)$ the point at infinity, and let $p_1,\dots,p_n$ be different rational points of $\mathbb{P}^1$, $p_i\neq p_0,p_\infty$. Let us define the divisors $D=p_1+\cdots+p_n$ and $G=rp_\infty-sp_0$, with

$$0\leq s\leq r<n.$$

Since $g=0$, the evaluation map $\alpha\colon L(G)\to\mathbb{F}_q(z)^n$ is injective, and $\mathcal{I}m\alpha$ defines a convolutional Goppa code $\mathcal{C}(D,G)$ of length n and dimension $k=r-s+1$.

Let us choose the functions $t^s,t^{s+1},\dots,t^r$ as a basis of $L(G)$. If $\alpha_i\in\mathbb{F}_q(z)$ is the local coordinate of the point p_i, $i=1,\dots,n$, the matrix of the evaluation map α is the following generator matrix for the code $\mathcal{C}(D,G)$:

$$G=\begin{pmatrix}\alpha_1^s & \alpha_2^s & \dots & \alpha_n^s\\ \alpha_1^{s+1} & \alpha_2^{s+1} & \dots & \alpha_n^{s+1}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_1^r & \alpha_2^r & \dots & \alpha_n^r\end{pmatrix}. \tag{7}$$

The dual convolutional Goppa code $\mathcal{C}^{\perp}(D,G)$ also has length n, and dimension $n-k=n-r+s-1$.

To construct $\mathcal{C}^{\perp}(D,G)$, let us choose in $L(K+D-G)$ the basis of rational differential forms

$$\left\langle\frac{dt}{t^s\prod_{i=1}^n(t-\alpha_i)},\frac{t\,dt}{t^s\prod_{i=1}^n(t-\alpha_i)},\dots,\frac{t^{n-r+s-2}dt}{t^s\prod_{i=1}^n(t-\alpha_i)}\right\rangle$$

and let us calculate the residues

$$\begin{aligned}&\mathrm{Res}_{p_j}\left(\frac{t^m\,dt}{t^s\prod_{i=1}^n(t-\alpha_i)}\right)\\ &=\mathrm{Res}_{p_j}\left(\frac{(t-\alpha_j+\alpha_j)^m d(t-\alpha_j)}{(t-\alpha_j)(t-\alpha_j+\alpha_j)^s\prod_{\substack{i=1\\ i\neq j}}^n(t-\alpha_j+\alpha_j-\alpha_i)}\right)\\ &=\frac{\alpha_j^m}{\alpha_j^s\prod_{\substack{i=1\\ i\neq j}}^n(\alpha_j-\alpha_i)}.\end{aligned}$$

If one sets

$$h_j=\frac{1}{\alpha_j^s\prod_{\substack{i=1\\ i\neq j}}^n(\alpha_j-\alpha_i)}$$

then the matrix H of $\beta\colon L(K+D-G)\to\mathbb{F}_q(z)^n$,

$$H=\begin{pmatrix}h_1 & h_2 & \cdots & h_n\\ h_1\alpha_1 & h_2\alpha_2 & \cdots & h_n\alpha_n\\ \vdots & \vdots & \ddots & \vdots\\ h_1\alpha_1^{n-r+s-2} & h_2\alpha_2^{n-r+s-2} & \dots & h_n\alpha_n^{n-r+s-2}\end{pmatrix} \tag{8}$$

is a generator matrix for the dual code $\mathcal{C}^{\perp}(D,G)$, and therefore a parity-check matrix for $\mathcal{C}(D,G)$. In fact, one has $H\cdot G^T=0$.

Remark 5.1: The matrix in (8) suggests that $\mathcal{C}^{\perp}(D,G)$ is an alternant code over the field $\mathbb{F}_q(z)$, and we can thus apply to $\mathcal{C}(D,G)$ some kind of Berlekamp–Massey decoding algorithm as a linear code over $\mathbb{F}_q(z)$.

Example 5.2: Let $a,b\in\mathbb{F}_q$ be two different nonzero elements, and

$$\alpha_i=a^{i-1}z+b^{i-1}, i=1,\dots,n,\ \text{with } n<q.$$

We present some examples of convolutional Goppa codes with canonical generator matrices [3], whose free distance d_{free} attains the generalized Singleton bound, i.e., they are MDS convolutional codes [8], and we include their encoding equations as linear systems

$$\left.\begin{aligned} z^{-1}s &= sA_{\delta\times\delta} + uB_{k\times\delta} \\ uG &= sC_{\delta\times n} + uD_{k\times n} \end{aligned}\right\}$$

where δ denotes the degree of the code (in the sense of [3].)

- Field $\mathbb{F}_3(z)$, $\mathbb{F}_3 = \{0,1,2\}$

$$\begin{aligned} G &= (z+1 \quad z+2) \\ H &= \begin{pmatrix} \dfrac{1}{2(z+1)} & \dfrac{1}{z+2} \end{pmatrix} \\ A &= (0), \quad B = (1), \quad C = (1 \quad 1), \quad D = (1 \quad 2) \end{aligned}$$

$$(n, k, \delta, d_{\text{free}}) = (2, 1, 1, 4).$$

- Field $\mathbb{F}_4(z)$, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where $\alpha^2 + \alpha + 1 = 0$

$$\begin{aligned} G &= \begin{pmatrix} 1 & 1 & 1 \\ z+1 & \alpha z + \alpha^2 & \alpha^2 z + \alpha \end{pmatrix} \\ H &= (\tfrac{1}{(\alpha^2 z+\alpha)(\alpha z+\alpha^2)} \quad \tfrac{1}{(\alpha^2 z+\alpha)(z+1)} \quad \tfrac{1}{(\alpha z+\alpha^2)(z+1)}) \\ A &= (0), \quad B = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ C &= (1 \quad \alpha \quad \alpha^2), \quad D = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \end{pmatrix} \end{aligned}$$

$$(n, k, \delta, d_{\text{free}}) = (3, 2, 1, 3).$$

- Field $\mathbb{F}_4(z)$

$$\begin{aligned} G &= (z+1 \quad z+\alpha \quad z+\alpha^2) \\ H &= \begin{pmatrix} \frac{1}{z+1} & \frac{\alpha}{z+\alpha} & \frac{\alpha^2}{z+\alpha^2} \\ 1 & \alpha & \alpha^2 \end{pmatrix} \\ A &= (0), \quad B = (1), \quad C = (1 \quad 1 \quad 1), \\ D &= (1 \quad \alpha \quad \alpha^2) \end{aligned}$$

$$(n, k, \delta, d_{\text{free}}) = (3, 1, 1, 6).$$

- Field $\mathbb{F}_5(z)$, $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

$$\begin{aligned} G &= ((z+1)^2 \quad (z+2)^2 \quad (z+4)^2) \\ H &= \begin{pmatrix} \frac{2}{(z+1)^2} & \frac{2}{(z+2)^2} & \frac{1}{(z+4)^2} \\ \frac{2}{z+1} & \frac{2}{z+2} & \frac{1}{z+4} \end{pmatrix} \\ A &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = (1 \quad 0) \\ C &= \begin{pmatrix} 2 & 4 & 3 \\ 1 & 1 & 1 \end{pmatrix}, \quad D = (1 \quad 4 \quad 1) \end{aligned}$$

$$(n, k, \delta, d_{\text{free}}) = (3, 1, 2, 9).$$

- Field $\mathbb{F}_5(z)$

$$\begin{aligned} G &= \begin{pmatrix} z+1 & 2z+3 & 4z+4 & 3z+2 \\ (z+1)^2 & (2z+3)^2 & (4z+4)^2 & (3z+2)^2 \end{pmatrix} \\ H &= \begin{pmatrix} \frac{4}{a^2bc} & \frac{4}{bcd^2} & \frac{4}{a^2bc} & \frac{4}{bcd^2} \\ \frac{4}{abc} & \frac{3}{bcd} & \frac{1}{abc} & \frac{2}{bcd} \end{pmatrix} \end{aligned}$$

where $a = z+1, b = z+2, c = z+3$ and $d = z+4$,

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 2 & 2 & 2 \\ 1 & 4 & 1 & 4 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \end{pmatrix}$$

$$(n, k, \delta, d_{\text{free}}) = (4, 2, 3, 8).$$

Remark 5.3: In the computation of free distance of these codes we do not take advantage of the fact that they are convolutional Goppa codes, as we explained in Section IV.

VI. CGC Associated With Elliptic Curves

We can obtain convolutional codes from elliptic curves in the same way. Let $X \subset \mathbb{P}^2_{\mathbb{F}_q(z)}$ be a plane elliptic curve over $\mathbb{F}_q(z)$, and let us denote by (x, y) the affine coordinates in $\mathbb{P}^2_{\mathbb{F}_q(z)}$. Let p_∞ be the infinity point, and $p_1, \ldots, p_n$ rational points of X, with $p_i = (x_i(z), y_i(z))$. Let us define $D = p_1 + \ldots + p_n$ and $G = rp_\infty$.

The "canonical" basis of $L(G)$ is $\{1, x, y, \ldots, x^a y^b\}$, with $2a + 3b = r$ (and $b = 0, 1$ so that there are no linear combinations). Thus, the evaluation map $\alpha\colon L(G) \to \mathbb{F}_q(z)^n$ is

$$\alpha(x^i y^j) = (x_1^i(z) y_1^j(z), \ldots, x_n^i(z) y_n^j(z)).$$

The image of a subspace $\Gamma \subseteq L(G)$ under the map α provides a Goppa convolutional code.

We present a couple of examples obtained from elliptic curves that, although not MDS, have free distance approaching that bound.

Example 6.1: We consider the curve over $\mathbb{F}_2(z)$

$$y^2 + (1+z)xy + (z+z^2)y = x^3 + (z+z^2)x^2$$

and the points

$$\begin{aligned} p_1 &= (z^2 + z, z^3 + z^2) \\ p_2 &= (0, z^2 + z) \\ p_3 &= (z, z^2). \end{aligned}$$

$L(G)$ is the subspace generated by $\{1, x\}$. Thus, the valuation map α is defined by the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ z^2 + z & 0 & z \end{pmatrix}.$$

This code has free distance $d_{\text{free}} = 2$. The maximum distance for its parameters is 3.

Example 6.2: Let us now consider the curve over $\mathbb{F}_2(z)$

$$y^2 + (1 + z + z^2)xy + (z^2 + z^3)y = x^3 + (z^2 + z^3)x^2$$

and the points

$$\begin{aligned} p_1 &= (z^3 + z^2, 0) \\ p_2 &= (0, z^3 + z^2) \\ p_3 &= (z^3 + z^2, z^5 + z^3) \\ p_4 &= (z^2 + z, z^3 + z) \\ p_5 &= (z^2 + z, z^4 + z^2). \end{aligned}$$

Again we take $L(G)$ as the subspace generated by $\{1, x\}$. Therefore, the valuation map α is defined by the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ z^3 + z^2 & 0 & z^3 + z^2 & z^2 + z & z^2 + z \end{pmatrix}.$$

This code has free distance $d_{\text{free}} = 4$. The maximum distance for its parameters is 5.

Remark 6.3: Every elliptic curve X over $\mathbb{F}_q(z)$ can be considered as the generic fiber of a fibration $\mathcal{X} \to U = \operatorname{Spec}\mathbb{F}_q[z]$, with some fibers singular curves of genus 1. The global structure of this fibration is related to the singular fibers (see [5]); the translation into the language of coding theory of the arithmetic and geometric properties of the fibration is the first step in the program of applying the general construction to the effective construction of good convolutional Goppa codes of genus 1.

Appendix

Let us consider a convolutional Goppa code $\mathcal{C}(D, G)$ of length n over a curve X defined over $\mathbb{F}_q(z)$ and let us assume that X can be extended to a family of curves X_U over $U = \mathrm{Spec}\mathbb{F}_q[z] = \mathbb{A}^1_{\mathbb{F}_q}$ (as in [4]).

Let X_0 be the fiber of X_U over the origin of U. The points $p_1, \ldots, p_n$ of the divisor D define sections $p_i(z)\colon \mathbb{A}^1_{\mathbb{F}_q} \to X_U$ and the polynomial words of the code $\mathcal{C}(D, G)$ are defined by evaluating the sections $s \in L(G)$ along the sections $p_i(z)$.

Let p be one of the points defined by D, C_p the curve of X_U defined as the image of the section $p(z)$ and q_0 the intersection of C_p with X_0, that is, $q_0 = p(0)$. Let us assume that $L(G)$ is a very ample linear series [6], and assume that X_U is immersed in $\mathbb{P}^N_{\mathbb{F}_q} \times \mathbb{P}^1_{\mathbb{F}_q}$ using the linear series $L(G)$. Let us denote by $\pi_r(q_0)$ the r-th osculating plane to the curve C_p at the point q_0. One has a sequence of strict inclusions

$$\pi_0(q_0) = q_0 \subset \pi_1(q_0) \subset \pi_2(q_0) \subset \ldots \subset \pi_r(q_0) \subset \cdots.$$

The evaluation of s at p, $s(p)$ can be expressed by

$$s(p) = s_0 + s_1 z + \cdots + s_n z^n$$

where $s_0 = s(0)$ and s_r, the rth coefficient, can be interpreted as the rth jet of $s(z)$ at the point q_0.

With this interpretation in mind, one has that $s_r = 0$ if and only if

$$H_s \cap \pi_r(q_0) \neq \emptyset \quad \text{and} \quad H_s \cap \pi_{r-1}(q_0) \subsetneqq H_s \cap \pi_r(q_0)$$

where H_s is the hyperplane defined by the section s.

Hence the problem of computing the number $\#\{r \mid s_r = 0\}$ can be translated into a problem of enumerative geometry over finite fields.

The main problem here is to develop the classical theory of osculating planes and all the classical computations in the case of finite base fields. This is not an easy problem but its solution would allow one to give a geometric interpretation of the free distance of convolutional Goppa codes.

Acknowledgment

The authors would like to thank J. Prada Blanco for helpful comments that served to stimulate our work.

References

[1] G. D. Forney Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inf. Theory*, vol. IT-16, no. 3, pp. 720–738, May 1970.

[2] P. Piret, *Convolutional Codes: An Algebraic Approach.* Cambridge, MA: MIT Press, 1988.

[3] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory Volume I.* Amsterdam, The Netherlands: North-Holland, 1998, pp. 1065–1138.

[4] J. A. D. Pérez, J. M. M. Porras, and G. S. Sotelo, "Convolutional codes of Goppa type," *Appl. Algebra Engrg. Comm. Comput.*, vol. 15, no. 1, pp. 51–61, 2004.

[5] J. Tate, "Algorithm for determining the type of a singular fiber in an elliptic pencil," in *Modular Functions of one Variable, IV (Proc. Int. Summer School, Univ. Antwerp, Antwerp, 1972) (Lecture Notes in Mathematics).* Berlin, Germany: Springer Verlag, 1975, vol. 476, pp. 33–52.

[6] R. Hartshorne, *Algebraic Geometry*, ser. Graduate Texts in Mathematics. New York: Springer-Verlag, 1977, vol. 52.

[7] J. Rosenthal, "Connections between linear systems and convolutional codes," in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999)*, ser. IMA Vol. Math. Appl.. New York: Springer-Verlag, 2001, vol. 123, pp. 39–66.

[8] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Appl. Algebra Eng. Commun. Comput.*, vol. 10, no. 1, pp. 15–32, 1999.

A General Framework for Codes Involving Redundancy Minimization

Michael B. Baer, *Member, IEEE*

***Abstract*—A framework with two scalar parameters is introduced for various problems of finding a prefix code minimizing a coding penalty function. The framework encompasses problems previously proposed by Huffman, Campbell, Nath, and Drmota and Szpankowski, shedding light on the relationships among these problems. In particular, Nath's range of problems can be seen as bridging the minimum average redundancy problem of Huffman with the minimum maximum pointwise redundancy problem of Drmota and Szpankowski. Using this framework, two linear-time Huffman-like algorithms are devised for the minimum maximum pointwise redundancy problem, the only one in the framework not previously solved with a Huffman-like algorithm. Both algorithms provide solutions common to this problem and a subrange of Nath's problems, the second algorithm being distinguished by its ability to find the minimum variance solution among all solutions common to the minimum maximum pointwise redundancy and Nath problems. Simple redundancy bounds are also presented.**

***Index Terms*—Huffman algorithm, minimax redundancy, optimal prefix code, Rényi entropy, unification.**

I. Introduction

A source emits symbols drawn from the alphabet $\mathcal{X} = \{1, 2, \ldots, n\}$. Symbol i has probability p_i, thus defining probability mass function vector $\boldsymbol{p}$. We assume without loss of generality that $p_i > 0$ for every $i \in \mathcal{X}$, and that $p_i \leq p_j$ for every $i > j (i, j \in \mathcal{X})$. The source symbols are coded into binary codewords. Each codeword c_i corresponding to symbol i has length l_i, thus defining length vector $\boldsymbol{l}$.

It is well known that Huffman coding [1] yields a prefix code minimizing $\sum_{i \in \mathcal{X}} p_i l_i$ given the natural coding constraints: the integer constraint, $l_i \in \mathbb{Z}_+$, and the Kraft (McMillan) inequality [2]

$$\sum_{i \in \mathcal{X}} 2^{-l_i} \leq 1.$$

Hu, Kleitman, and Tamaki [3] and Parker [4] independently examined other cases in which Huffman-like algorithms were optimal; this work was later extended [5], [6]. Other modifications of the Huffman coding problem were considered in analytical papers [7]–[9], although none of these proposed a Huffman-like algorithmic solution. In each paper, relationships between the modified problem and the Huffman coding problem were explored. Parker proposed an algorithmically motivated two-function parameterization defining various Huffman

Manuscript received February 13, 2003; revised October 3, 2005. This work was supported in part by the National Science Foundation under Grant CCR-9973134 and the Multidisciplinary University Research Initiative (MURI) under Grant DAAD-19-99-1-0215.

The author was with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305-9505 USA. He is now with Electronics for Imaging, Foster City, CA 94404 USA (e-mail: Michael.Baer@efi.com).

Communicated by S. A. Savari, Associate Editor for Source Coding.
Digital Object Identifier 10.1109/TIT.2005.860469